

Technische und organisatorische Maßnahmen Auftragsverarbeiter § 28 DSGVO

MC Arztsysteme Rheinland GmbH
 Römmerskirchener Str.216
 50259 Pulheim

1. Zutrittskontrolle

Maßnahmen, die geeignet sind, Unbefugten den Zutritt zu Datenverarbeitungsanlagen, mit denen personenbezogene Daten verarbeitet oder genutzt werden, zu verwehren.

- | | |
|---|--|
| <input type="checkbox"/> Alarmanlage | <input checked="" type="checkbox"/> Absicherung von Gebäudeschächten |
| <input type="checkbox"/> Automatisches Zugangskontrollsystem | <input type="checkbox"/> Chipkarten-/Transponder-Schließsystem |
| <input type="checkbox"/> Schließsystem mit Codesperre | <input checked="" type="checkbox"/> Manuelles Schließsystem |
| <input type="checkbox"/> Biometrische Zugangssperren | <input type="checkbox"/> Videoüberwachung der Zugänge |
| <input type="checkbox"/> Lichtschranken / Bewegungsmelder | <input checked="" type="checkbox"/> Sicherheitsschlösser |
| <input checked="" type="checkbox"/> Schlüsselregelung (Schlüsselausgabe etc.) | <input type="checkbox"/> Personenkontrolle beim Pförtner / Empfang |
| <input type="checkbox"/> Protokollierung der Besucher | <input checked="" type="checkbox"/> Sorgfältige Auswahl von Reinigungspersonal |
| <input type="checkbox"/> Sorgfältige Auswahl von Wachpersonal | <input type="checkbox"/> Tragepflicht von Berechtigungsausweisen |

2. Zugangskontrolle

Maßnahmen, die geeignet sind zu verhindern, dass Datenverarbeitungssysteme von Unbefugten genutzt werden können.

- | | |
|--|---|
| <input checked="" type="checkbox"/> Zuordnung von Benutzerrechten | <input checked="" type="checkbox"/> Erstellen von Benutzerprofilen |
| <input checked="" type="checkbox"/> Passwortvergabe | <input type="checkbox"/> Authentifikation mit biometrischen Verfahren |
| <input checked="" type="checkbox"/> Authentifikation mit Benutzername / Passwort | <input checked="" type="checkbox"/> Zuordnung von Benutzerprofilen zu IT-Systemen |
| <input type="checkbox"/> Gehäuseverriegelungen | <input checked="" type="checkbox"/> Einsatz von VPN-Technologie |
| <input type="checkbox"/> Sperren von externen Schnittstellen (USB etc.) | <input checked="" type="checkbox"/> Sicherheitsschlösser |
| <input checked="" type="checkbox"/> Schlüsselregelung (Schlüsselausgabe etc.) | <input type="checkbox"/> Personenkontrolle beim Pförtner / Empfang |
| <input type="checkbox"/> Protokollierung der Besucher | <input checked="" type="checkbox"/> Sorgfältige Auswahl von Reinigungspersonal |
| <input type="checkbox"/> Sorgfältige Auswahl von Wachpersonal | <input type="checkbox"/> Tragepflicht von Berechtigungsausweisen |
| <input type="checkbox"/> Einsatz von Intrusion-Detection-Systemen | <input type="checkbox"/> Verschlüsselung von mobilen Datenträgern |

Erstellt von: Stefan Breitkopf	Freigegeben von: Davor Zepic	Geprüft von: Davor Zepic
Erstellt am: 19.03.2018	Freigegeben am: 22.05.2018	Geprüft am: 22.05.2018
Version: 2	Seite 1 von 4	Letzte Änderung am: 22.05.2018

- | | |
|---|--|
| <input checked="" type="checkbox"/> Einsatz von Anti-Viren-Software | <input type="checkbox"/> Verschlüsselung von Datenträgern in Laptops / Notebooks |
| <input checked="" type="checkbox"/> Einsatz einer Hardware-Firewall | <input checked="" type="checkbox"/> Einsatz einer Software-Firewall |

3. Zugriffskontrolle

Maßnahmen, die gewährleisten, dass die zur Benutzung eines Datenverarbeitungssystems Berechtigten ausschließlich auf die ihrer Zugriffsberechtigung unterliegenden Daten zugreifen können, und dass personenbezogene Daten bei der Verarbeitung, Nutzung und nach der Speicherung nicht unbefugt gelesen, kopiert, verändert oder entfernt werden können.

- | | |
|--|---|
| <input checked="" type="checkbox"/> Erstellen eines Berechtigungskonzepts | <input checked="" type="checkbox"/> Verwaltung der Rechte durch Systemadministrator |
| <input checked="" type="checkbox"/> Anzahl der Administratoren auf das „Notwendigste“ reduziert | <input checked="" type="checkbox"/> Passworrichtlinie inkl. Passwortlänge, Passwortwechsel |
| <input checked="" type="checkbox"/> Protokollierung von Zugriffen auf Anwendungen, insbesondere bei der Eingabe, Änderung und Löschung von Daten | <input checked="" type="checkbox"/> Sichere Aufbewahrung von Datenträgern |
| <input checked="" type="checkbox"/> physische Löschung von Datenträgern vor Wiederverwendung | <input checked="" type="checkbox"/> ordnungsgemäße Vernichtung von Datenträgern (DIN 32757) |
| <input checked="" type="checkbox"/> Einsatz von Aktenvernichtern bzw. Dienstleistern (nach Möglichkeit mit Datenschutz-Gütesiegel) | <input checked="" type="checkbox"/> Protokollierung der Vernichtung |
| <input checked="" type="checkbox"/> Verschlüsselung von Datenträgern | |

4. Weitergabekontrolle

Maßnahmen, die gewährleisten, dass personenbezogene Daten bei der elektronischen Übertragung oder während ihres Transports oder ihrer Speicherung auf Datenträger nicht unbefugt gelesen, kopiert, verändert oder entfernt werden können, und dass überprüft und festgestellt werden kann, an welche Stellen eine Übermittlung personenbezogener Daten durch Einrichtungen zur Datenübertragung vorgesehen ist.

- | | |
|---|---|
| <input checked="" type="checkbox"/> Einrichtungen von Standleitungen bzw. VPN-Tunneln | <input type="checkbox"/> Weitergabe von Daten in anonymisierter oder pseudonymisierter Form |
| <input type="checkbox"/> E-Mail-Verschlüsselung | <input type="checkbox"/> Erstellen einer Übersicht von regelmäßigen Abruf- und Übermittlungsvorgängen |
| <input type="checkbox"/> Dokumentation der Empfänger von Daten und der Zeitspannen der geplanten Überlassung bzw. vereinbarter Löschrufen | <input type="checkbox"/> Beim physischen Transport: sichere Transportbehälter/-verpackungen |

Erstellt von: Stefan Breitkopf	Freigegeben von: Davor Zepic	Geprüft von: Davor Zepic
Erstellt am: 19.03.2018	Freigegeben am: 22.05.2018	Geprüft am: 22.05.2018
Version: 2	Seite 2 von 4	Letzte Änderung am: 22.05.2018

Eingabekontrolle

Maßnahmen, die gewährleisten, dass nachträglich überprüft und festgestellt werden kann, ob und von wem personenbezogene Daten in Datenverarbeitungssysteme eingegeben, verändert oder entfernt worden sind.

- | | |
|---|--|
| <input checked="" type="checkbox"/> Protokollierung der Eingabe, Änderung und Löschung von Daten | <input type="checkbox"/> Erstellen einer Übersicht, aus der sich ergibt, mit welchen Applikationen welche Daten eingegeben, geändert und gelöscht werden können. |
| <input checked="" type="checkbox"/> Nachvollziehbarkeit von Eingabe, Änderung und Löschung von Daten durch individuelle Benutzernamen (nicht Benutzergruppen) | <input checked="" type="checkbox"/> Aufbewahrung von Formularen, von denen Daten in automatisierte Verarbeitungen übernommen worden sind |
| <input checked="" type="checkbox"/> Vergabe von Rechten zur Eingabe, Änderung und Löschung von Daten auf Basis eines Berechtigungskonzepts | |

5. Auftragskontrolle

Maßnahmen, die gewährleisten, dass personenbezogene Daten, die im Auftrag verarbeitet werden, nur entsprechend den Weisungen des Auftraggebers verarbeitet werden können.

- | | |
|--|---|
| <input checked="" type="checkbox"/> Auswahl des Auftragnehmers unter Sorgfaltsgesichtspunkten (insbesondere hinsichtlich Datensicherheit) | <input type="checkbox"/> vorherige Prüfung der und Dokumentation der beim Auftragnehmer getroffenen Sicherheitsmaßnahmen |
| <input checked="" type="checkbox"/> schriftliche Weisungen an den Auftragnehmer (z.B. durch Auftragsdatenverarbeitungsvertrag) i.S.d. § 11 Abs. 2 BDSG | <input checked="" type="checkbox"/> Verpflichtung der Mitarbeiter des Auftragnehmers auf das Datengeheimnis und die Bestimmungen der § 203 StGB |
| <input checked="" type="checkbox"/> Auftragnehmer hat Datenschutzbeauftragten bestellt falls gesetzlich erforderlich | <input checked="" type="checkbox"/> Sicherstellung der Vernichtung von Daten nach Beendigung des Auftrags |
| <input checked="" type="checkbox"/> Wirksame Kontrollrechte gegenüber dem Auftragnehmer vereinbart | <input checked="" type="checkbox"/> laufende Überprüfung des Auftragnehmers und seiner Tätigkeiten |
| <input checked="" type="checkbox"/> Vertragsstrafen bei Verstößen | |

6. Verfügbarkeitskontrolle

Maßnahmen, die gewährleisten, dass personenbezogene Daten gegen zufällige Zerstörung oder Verlust geschützt sind.

- | | |
|---|--|
| <input checked="" type="checkbox"/> Unterbrechungsfreie Stromversorgung (USV) | <input type="checkbox"/> Klimaanlage in Serverräumen |
| <input type="checkbox"/> Geräte zur Überwachung von Temperatur und Feuchtigkeit in Serverräumen | <input checked="" type="checkbox"/> Schutzsteckdosenleisten in Serverräumen |
| <input type="checkbox"/> Feuer- und Rauchmeldeanlagen | <input checked="" type="checkbox"/> Feuerlöschgeräte in Serverräumen |
| <input type="checkbox"/> Alarmmeldung bei unberechtigten Zutritten zu Serverräumen | <input checked="" type="checkbox"/> Erstellen eines Backup- & Recoverykonzepts |
| <input checked="" type="checkbox"/> Testen von Datenwiederherstellung | <input checked="" type="checkbox"/> Erstellen eines Notfallplans |

Erstellt von: Stefan Breitkopf	Freigegeben von: Davor Zepic	Geprüft von: Davor Zepic
Erstellt am: 19.03.2018	Freigegeben am: 22.05.2018	Geprüft am: 22.05.2018
Version: 2	Seite 3 von 4	Letzte Änderung am: 22.05.2018

Aufbewahrung von Datensicherung an einem sicheren, ausgelagerten Ort

 Serverräume nicht unter sanitären Anlagen

7. Trennungsgebot

Maßnahmen, die gewährleisten, dass zu unterschiedlichen Zwecken erhobene Daten getrennt verarbeitet werden können.

 physikalisch getrennte Speicherung auf gesonderten Systemen oder Datenträgern

 Logische Mandantentrennung (softwareseitig)

 Erstellung eines Berechtigungskonzepts

 Verschlüsselung von Datensätzen, die zu demselben Zweck verarbeitet werden

 Versehen der Datensätze mit Zweckattributen/Datenfeldern

 Bei pseudonymisierten Daten: Trennung der Zuordnungsdatei und der Aufbewahrung auf einem getrennten, abgesicherten IT-System

 Festlegung von Datenbankrechten

 Trennung von Produktiv- und Testsystem

Datenschutzbeauftragter:

Stefan Breitkopf

Bereichsleitung IT-Sicherheit und Datenschutz
 Westernstr 2
 31655 Stadthagen
 Email: dsb@arztsysteme-rheinland.de

IT-Verantwortlicher:

Carsten Voss

Bereichsleitung Projekte und interne IT
 Römmerskirchener Str.21
 650259 Pulheim
 Email: c.voss@arztsysteme-rheinland.de

Geschäftsführer:

Davor Zepic

Geschäftsführung
 Römmerskirchener Str.21
 650259 Pulheim
 Email: d.zepic@arztsysteme-rheinland.de

Die internen Anweisungen der ASR im Hinblick auf Datenschutz und Datensicherheit sind im QM-System der ASR dargelegt. Eine Versionierung findet statt. Die Datenschutzbeauftragten von Auftraggebern sind berechtigt, relevante Dokumente bei der ASR einzusehen. Dazu wenden Sie sich bitte an unseren Datenschutzbeauftragten. Im Übrigen werden diese Dokumente aus Sicherheitsgründen geheim gehalten.

Hiermit erkläre ich, dass ich die vorgenannten Maßnahmen im Hinblick auf die Art der betroffenen personenbezogenen Daten für ausreichend halte und dass die ASR diese Maßnahmen nach meinen Erkundungen und Wissen implementiert hat.

Stadthagen, 19.05.2018

Stefan Breitkopf, Datenschutzbeauftragter der ASR GmbH

Erstellt von: Stefan Breitkopf	Freigegeben von: Davor Zepic	Geprüft von: Davor Zepic
Erstellt am: 19.03.2018	Freigegeben am: 22.05.2018	Geprüft am: 22.05.2018
Version: 2	Seite 4 von 4	Letzte Änderung am: 22.05.2018